CLAIM AMENDMENTS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

~~storing at least one key within a tamper detection boundary of a circuit card coupled to a system bus of a host processor;~~

storing encrypted metadata for determining a configuration of a redundant array of independent disks (RAID) storage;

receiving a request to write data to one or more locations in the RAID storage;

encrypting, based upon [[the]] at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in the one or more locations of the RAID storage ~~in a storage coupled to the system bus, the encrypted write data generated by an input/output ("I/O") processor on the circuit card~~;

generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the RAID storage; and

selecting the one or more locations in the RAID storage for storing the one or more respective portions of the encrypted write data by translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the RAID storage.

2. (Currently Amended) The method of claim 1, wherein[[:]]

~~the storage comprises a redundant array of independent disks (RAID); and~~

the check data comprises one of parity data and a copy of the encrypted write data.

3. (Currently Amended) The method of claim 1~~, further comprising:~~

~~in response to an attempt to tamper with the at least one key, erasing the at least one key~~ wherein the configuration of the RAID storage comprises an address or a mapping table including a location in the RAID storage for the encrypted write data to be stored.

4. (Currently Amended) The method of claim 1, further comprising[[:]]

~~determining, based upon one or more credentials, whether to permit execution of one or more operations involving the storage~~ decomposing the write data into the one or more portions before encrypting the one or more respective portions of the write data, the one or more portions to correspond to one or more stripes to be written into the RAID storage.

5. (Currently Amended) A method comprising:

storing encrypted metadata for determining a configuration of a redundant array of independent disks (RAID) storage;

receiving a request to retrieve requested data from one or more locations in the RAID storage;

translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata;

~~receiving a read request from a host processor;~~

retrieving one or more respective portions of encrypted data from ~~a plurality of storage devices comprised~~ the one or more translated locations in [[a]] the RAID storage ~~coupled to the host processor~~; and

decrypting~~, based upon at least one key stored within a tamper detection boundary of an encryption device coupled to the host processor,~~ the one or more respective portions of the encrypted read data retrieved from the storage based upon at least one key to generate one or more respective portions of read data~~, the read data generated by an input/output ("I/O") processor located within the tamper detection boundary of the encryption device~~.

6. (Currently Amended) The method of claim 5~~, further comprising:~~

~~prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized~~ wherein the configuration of the RAID storage comprises an address or a mapping table including a location in the RAID storage where the encrypted read data is stored.

7. (Previously Presented) The method of claim 6, further comprising:

generating the at least one key based upon at least one of one or more tokens and one or more passwords.

8. (Currently Amended) The method of claim 5[[,]] wherein[[:]]

~~the storage also stores metadata; and the method~~ further ~~comprises~~ comprising encrypting [[the]] metadata to generate the encrypted metadata based upon the at least one key.

9. (Currently Amended) The method of claim 8, wherein[[:]]the metadata comprises partition information.

10. (Currently Amended) An apparatus comprising:

circuitry to receive a request to write data to one or more locations in the RAID storage;

the circuitry also being capable of:

storing encrypted metadata for determining a configuration of a redundant array of independent disks (RAID) storage;

encrypting, based upon at least one key ~~stored within a tamper detection boundary~~, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in the RAID storage;

~~the circuitry also being capable of:~~

generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the storage; and

selecting the one or more locations in the RAID storage for storing the one or more respective portions of the encrypted write data by translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the RAID storage.

11. (Currently Amended) The apparatus of claim 10, wherein[[:]]

~~the storage comprises a redundant array of independent disks (RAID); and~~

the check data comprises one of parity data and a copy of the encrypted write data.

12. (Previously Presented) The apparatus of claim 10, wherein:

the circuitry is also capable of storing the at least one key in memory; and

in response to an attempt to tamper with the at least one key, erasing the at least one key from the memory.

13. (Currently Amended) The apparatus of claim 10, wherein:

the circuitry is also capable of determining, based upon one or more credentials, whether to permit execution of one or more operations involving the RAID storage.

14. (Currently Amended) The apparatus of claim 10, further comprising:

circuitry to receive a read request, retrieve one or more respective portions of the encrypted data from the ~~plurality of~~ storage devices comprised in the RAID storage and decrypting, based upon the at least one key, one or more respective portions of the encrypted read data retrieved from the RAID storage to generate one or more respective portions of read data.

15. (Previously Presented) The apparatus of claim 14, wherein the circuitry is also capable of:

prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized.

16. (Previously Presented) The apparatus of claim 15, wherein:

the circuitry is also capable of generating the at least one key based upon at least one of one or more tokens and one or more passwords.

17. (Currently Amended) The apparatus of claim 14, wherein[[:]]

~~the storage also stores metadata; and~~ the circuitry is also capable of encrypting [[the]] metadata to generate the encrypted metadata based upon the at least one key.

18. (Original) The apparatus of claim 17, wherein:

the metadata comprises partition information.

19. (Currently Amended) ~~An article comprising a~~ A tangible machine-readable storage medium having stored therein instructions that when executed by a machine result in the following:

~~storing at least one key within a tamper detection boundary of a circuit card coupled to a system bus of a host processor;~~

storing encrypted metadata for determining a configuration of a redundant array of independent disks (RAID) storage;

receiving a request to write data to one or more locations in the RAID storage;

encrypting, based upon [[the]] at least one key, one or more respective portions of the write data to generate one or more respective portions of encrypted write data to be stored in the one or more locations of the RAID storage ~~in a storage coupled to the system bus, the encrypted write data generated by an input/output ("I/O") processor on the circuit card~~;

generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the RAID storage; and selecting the one or more

locations in the RAID storage for storing the one or more respective portions of the encrypted write data by translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the RAID storage.

20. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 19, wherein:

~~the storage comprises a redundant array of independent disks (RAID); and~~

the check data comprises one of parity data and a copy of the encrypted write data.

21. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 19, wherein the instructions when executed by the machine also result in:

storing the at least one key in memory; and

in response to an attempt to tamper with the at least one key, erasing the at least one key.

22. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 19, wherein the instructions when executed by the machine also result in:

determining, based upon one or more credentials, whether to permit execution of one or more operations involving the RAID storage.

23. (Currently Amended) ~~An article comprising a~~ A tangible machine-readable storage medium having stored therein instructions that when executed by a machine result in the following:

storing encrypted metadata for determining a configuration of a redundant array of independent disks (RAID) storage;

receiving a request to retrieve requested data from one or more locations in the RAID storage;

translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata;

~~receiving a read request from a host processor;~~

retrieving one or more respective portions of encrypted data from ~~a plurality of storage devices comprised~~ the one or more translated locations in [[a]] the RAID storage ~~coupled to the host processor~~; and

decrypting~~, based upon at least one key stored within a tamper detection boundary of an encryption device coupled to the host processor,~~ the one or more respective portions of the encrypted read data retrieved from the storage based upon at least one key to generate one or more respective portions of read data~~, the read data generated by an input/output ("I/O") processor located within the tamper detection boundary of the encryption device~~.

24. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 23, wherein the instructions when executed by the machine also result in:

prior to the decrypting of the one or more respective portions of the encrypted data, determining, based upon one or more credentials, whether the request is authorized.

25. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 24, wherein the instructions when executed by the machine also result in:

generating the at least one key based upon at least one of one or more tokens and one or more passwords.

26. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 23, wherein[[:]]~~the storage also stores metadata; and~~ the instructions when executed by the machine also result in encrypting [[the]] metadata to generate the encrypted metadata based upon the at least one key.

27. (Currently Amended) The ~~article~~ tangible machine-readable storage medium of claim 26, wherein:

the metadata comprises partition information.

28. (Currently Amended) A system comprising:

a circuit board comprising a circuit card slot and a circuit card that is capable of being inserted into the circuit card slot, the circuit card comprising circuitry, the circuitry being capable of encrypting, based upon at least one key, one or more respective portions of write data to generate one or more respective portions of encrypted write data to be stored in one or more locations in a redundant array of independent disks (RAID) storage,

wherein the circuitry also is capable of:

storing encrypted metadata for determining a configuration of the RAID storage;

receiving a request to write data to one or more locations in the RAID storage;

generating, based upon the one or more respective portions of the encrypted write data, check data to be stored in the RAID storage; and

selecting the one or more locations by translating the one or more locations specified in the request into one or more physical or logical locations in the RAID storage based at least upon the stored encrypted metadata so as to permit the one or more respective portions of the encrypted write data to be distributed among two or more storage devices comprised in the RAID storage[[,]] ~~wherein the circuit comprises: an input/output (I/O) processor, and non-volatile memory that is capable of storing the at least one key, wherein the circuitry is capable of detecting an attempt to tamper with the at least one key, and in response to the attempt, erasing the at least one key from the memory~~.

29. (Cancelled)

30. (Previously Presented) The system of claim 28, wherein the circuit board also comprises:

a host processor coupled to the circuit card slot via a bus;

one or more token memories to store one or more tokens; and

additional circuitry to read one or more additional tokens stored in a removable token memory after the removable token memory is inserted into a token reader.

31. – 33. (Cancelled)